Задание выполнил студент группы 2345 Романенко Кирилл

Дано: К Вам за аудитом ИБ обратился владелец Интернет-ресурса, на котором пользователи:

- Размещают свои личные объявления, в т.ч. загружают файлы и фотографии
- Обмениваются контактными данными
- Не проводятся платежи

Урок 1. Область и критерии аудита

1. Составьте список доп. вопросов, чтобы определить критерии аудита ИБ

Сколько локаций затрагивает Интернет-ресурс (хостинг, обслуживание); Сколько человек его обслуживает (ИТ и ИБ); Какой состав ИТ-инфраструктуры (узлы и их кол-во); Есть ли аутсорсинг; Есть ли локальные акты по ИБ; Есть ли ограничения по времени?

2. Определите подходящие критерии аудита ИБ

Локальные акты (если есть); Требования по линии персональных данных (ФЗ-152, ПП РФ № 1119); Контроли из ISO/IEC 27001 (прил. А); OWASP Top Ten Proactive Controls 2018; Отсутствие уязвимостей из OWASP Top 10

3. Определите область аудита ИБ

Локации (хостинг, обслуживание); Разработчики, ИТ и ИБ персонал, аутсорсеры (если есть); Процессы обработки и обеспечения ИБ; Серверное оборудование, АРМ персонала, СЗИ; Время

Урок 2. План аудита и состав группы

1. Составьте список доп. вопросов, чтобы составить план аудита ИБ и определить состав группы по аудиту ИБ

Какие каналы взаимодействия можно использовать, в т.ч. вопросы конфиденциальности;
Наличие интервьюируемых лиц в период проведения аудита ИБ и их роли;
Наличие сопровождающих лиц: какие условия будут предоставлены аудиторам (помещения, доступ к системам, документации и тл)?

2. Подготовьте план аудита ИБ (таблица)

№	Наименование этапа	Дата начала	Длительность, раб.дни	Примечание
1	Предварительное совещание	04.04.23	0,125	1 час
2	Получение документации	05.03.23	2	
3	Анализ полученной документации	10.03.23	2	
4	Проведение интервью	12.04.23	5	Длительность 1 интервью = 45 мин
5	Использование инструментальных средств	12.04.23	5	
6	Подготовка отчёта	19.04.23	5	
7	Заключительное совещание	25.04.23		

3. Определите состав группы по аудиту ИБ (исключительный и ролевой состав)

Руководитель группы по аудиту ИБ;
Аудитор по линии персональных данных;
Аудитор по линии ISO/IEC 27001 и OWASP Top Ten Proactive Controls 2018;
Тех. эксперт по OWASP Top 10

Урок 3. Как проводить аудит информационной безопасности?

1. Какие способы сбора информации Вы бы использовали (список)?

- Проведение интервью с разработчиками, ИТ и ИБ специалистами
- Опросные листы для аутсорсинга
- Анализ документации
- Показатели тех.средств

2. Какие свидетельства Вы могли бы получить (список)?

- Записи аудиторов
- Заполненные опросные листы
- Документы
- Данные тех.средств

Урок 4. Как завершить аудит информационной безопасности?

- Заключительное совещание
- Подготовка отчёта с опорой на стандарты с требованиями к его формату и содержанию:
  1. ISO 19011:2018
  2. Положение № 382-П
  3. СТО БР ИББС-1.1-2007
  4. ГОСТ Р 57580.2-2018
  5. Рекомендации от BSI
  6. Рекомендации от ISACA